United States General Accounting Office

GAO

Report to the Ranking Minority Member, Committee on Energy and Commerce, House of Representatives

July 2001

INFORMATION SYSTEMS

Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security

GAO-01-863

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	7/1/2001	Report 7/1/2001

4. TITLE AND SUBTITLE
Information Systems: Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security

5. FUNDING NUMBERS

6. AUTHOR(S)
GAO

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Booz Allen & Hamilton
8283 Greensboro Drive
McLean, VA 22102

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Unites States General
Accounting Office
Washington, DC

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited..

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 Words)*

The various components of SEC’s ARP program provide it with a reasonable level of assurance that the SROs address capacity, security, and other information system issues. However, SEC’s ARP oversight could be improved. To plan and conduct inspections of SRO systems issues, ARP staff use various criteria, including checklists that are based on ARP policy statements and standards from guidance developed by other external audit organizations and information echnology bodies, such as banking regulators. However, we found that the ARP program has not consolidated these criteria into a single guide that covers all the issues key to SEC oversight or that provides the specific review steps.

14. SUBJECT TERMS
IATAC Collection, information security

15. NUMBER OF PAGES
39

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Contents

Abbreviations

ARP Automation Review Policy
ECN electronic communication network
NASD National Association of Securities Dealers
SEC Securities and Exchange Commission
SRO self-regulatory organizations

GAO
Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

July 25, 2001

The Honorable John D. Dingell
Ranking Minority Member
Committee on Energy and Commerce
House of Representatives

Dear Mr. Dingell:

This report responds to your April 11, 2000, request that we assess the effectiveness of the Securities and Exchange Commission's (SEC) oversight of capacity planning and security procedures for information systems at the securities and options exchanges and clearing organizations. These systems are essential to the orderly functioning of the U.S. securities markets, which have become increasingly important to our economy. In recent years, capacity-related problems and other disruptions involving the exchanges have resulted in processing delays within the national market system. These exchanges and clearing organizations also need stringent security measures for their information systems to prevent unwarranted access by hackers and other unauthorized users who could disrupt or otherwise compromise the integrity of the markets. To address these concerns, in 1989, SEC created its Automation Review Policy (ARP) program, which calls for the exchanges and clearing organizations that act as self-regulatory organizations (SRO) to voluntarily follow SEC guidance and submit to oversight of their information systems.[1] Key components of the ARP program include two policy statements that provide voluntary guidelines to the SROs, periodic on-site inspections by SEC staff, and independent reviews of SRO systems by internal auditors or external organizations. In addition, SROs are expected to provide SEC with reports of system outages and notices of system modifications.

As agreed with your staff, this report assesses the adequacy of SEC's oversight of information system capacity planning and security procedures at the stock and options exchanges and other SROs. Specifically, this report presents our assessment of key components of SEC oversight,

[1]The stock and options exchanges, such as the New York Stock Exchange and Chicago Board Options Exchange, and the clearing organizations, such as the National Securities Clearing Corporation and the Depository Trust Company, act as self-regulatory organizations to ensure that their members comply with their own rules and those of the securities laws.

including the (1) criteria and guidance SEC uses to conduct capacity planning and security inspections, (2) scope and frequency of SEC's inspections of SROs' information systems, (3) scope and frequency of the independent reviews of various aspects of the SROs' information systems, and (4) effect of the ARP program's voluntary nature on SEC oversight.

Results in Brief

The various components of SEC's ARP program provide it with a reasonable level of assurance that the SROs address capacity, security, and other information system issues. However, SEC's ARP oversight could be improved. To plan and conduct inspections of SRO systems issues, ARP staff use various criteria, including checklists that are based on ARP policy statements and standards from guidance developed by other external audit organizations and information technology bodies, such as banking regulators. However, we found that the ARP program has not consolidated these criteria into a single guide that covers all the issues key to SEC oversight or that provides the specific review steps. This lack of a consolidated inspection guide creates potential for inconsistency in SEC's oversight and creates a dependency on the knowledge and efforts of the individual ARP program staff, which has turned over frequently and has many inexperienced members.

Our review of the inspection reports and supporting work papers prepared by SEC staff indicated that, overall, SEC's inspections addressed the key areas of ARP guidance and often contained substantive recommendations designed to improve the SROs' procedures. Although SEC staff stated that the ARP program has no formal goal, the inspections were not being done as frequently as they would have preferred. The ARP program has a high turnover rate among its small staff. In addition, the program has had to oversee various lengthy, industrywide information system initiatives, such as the industry's preparations for the Year 2000 date change and more recently the transition to decimal prices for securities. As a result, ARP staff have conducted on-site inspections at most SROs only once every 2 or 3 years, and some of these inspections lasted only 1 day.

Although the ARP program initially called for SROs to have annual independent reviews that were expected to be conducted by external organizations, these reviews are now done mostly by SRO internal auditors. After the SROs raised concerns about the cost of using external organizations, SEC agreed to allow SROs to use either their own internal audit processes or external organizations to conduct the independent reviews. These internal audits are performed cyclically based on an annual risk analysis. SEC staff stated that they believed the SROs' internal audits

addressed the important ARP guidance areas over time. However, in at least five recent cases, SEC staff has recommended that SRO systems be reviewed by external organizations because either the SROs' internal auditors were not adequately addressing capacity issues, or the SEC staff identified a deficiency in the SROs' systems and procedures.

SEC staff stated that the SROs generally complied with the voluntary ARP program. Nevertheless, we found that significant ARP staff recommendations and concerns about capacity and security weaknesses were not being implemented or addressed. In addition, SROs were not always making the reports or notices requested under the ARP guidelines. Because the ARP policy statements established only voluntary guidelines, SROs not implementing ARP recommendations or creating requested reports or notices cannot be sanctioned under the ARP program. SEC officials said that they believed they could bring an official action against an SRO if they considered its failure to follow ARP serious enough to represent a violation of the general SEC requirement that exchanges be able to conduct day-to-day operations. However, the SEC staff said that the provision they cited has rarely if ever been used by SEC. When the voluntary program was established, SEC stated that it would consider making the program mandatory if concerns arose over the SROs' level of voluntary compliance. However, SEC has not developed criteria and performed a formal assessment of SRO compliance with the ARP program. In at least one case, an SRO that did not implement SEC's capacity-related recommendations later experienced problems with its systems that adversely affected the markets. We also identified additional examples of SROs that had not addressed SEC ARP staff recommendations and concerns over the lack of adequate backup trading facilities or recovery plans. The SROs are also to report systems outages to SEC and provide notice of modifications to their systems. SEC received such reports and notices from the SROs in many cases, but SEC staff said that they did not receive them for all events or changes, which makes planning for oversight more difficult.

This report includes recommendations to the Acting Chairman, SEC, that are designed to increase the effectiveness of SEC oversight of the SRO information systems that are critical to the orderly functioning of the markets. We obtained comments on a draft of this report from SEC. SEC disagreed with our recommendations and noted that activities it currently performs already address our recommendations' objectives. However, the activities SEC described have not resulted in the outcomes our recommendations are designed to achieve. SEC's comments are discussed near the end of this letter, and its written comments appear in appendix I.

Background

SEC introduced its ARP program in 1989 because of capacity and other problems in the exchanges' and clearing organizations' information systems. The program resulted from SEC's November 1989 policy statement that noted that many exchanges and other organizations experienced problems in their systems during the high trading volumes that occurred in October 1987 and again in October 1989.[2] This policy statement also cited disasters, such as fires or earthquakes, that required exchanges to implement their contingency planning procedures. Since the ARP program was created, exchanges, clearing organizations, and the systems that link the stock and options markets[3] have continued to periodically experience capacity-related problems or other disruptions.

Under the ARP program, SEC called on the SROs to ensure that the information technology systems they use to conduct market operations have adequate processing capacity for current and future estimated trading volumes. In addition, SEC sought assurances that SROs were taking steps to assess the risk to their operations from internal and external threats, such as unauthorized use, computer vandalism, or computer viruses. The first ARP policy statement called on the SROs to establish capacity planning procedures to estimate current and future information system capacity needs and to periodically conduct capacity stress tests. In addition, the statement recommended that the SROs have assessments performed of their systems capacity and their vulnerability to physical threat. In a second policy statement issued in May 1991, SEC provided more specific guidelines to the SROS that identified five primary areas it expected the SROs to have reviewed, including the general controls and security relating to computer operations and facilities, telecommunications, systems development, capacity planning and testing, and contingency planning.[4] The ARP program is administered by staff in SEC's Office of Technology and Enforcement within the Division of Market Regulation.

[2]Automated Systems of Self-Regulatory Organizations, Release No. 34-27445 (November 16, 1989), 54 Fed. Reg. 48703.

[3]Although not technically SROs, SEC's ARP program also oversees the Consolidated Tape Association, which administers systems that transmit information between the stock exchanges and Nasdaq, and the Options Price Reporting Authority, which administers a system that transmits information between the options markets.

[4]Automated Systems of Self-Regulatory Organizations, Release No. 34-29185, (May 9, 1991), 56 Fed. Reg. 22490.

Scope and Methodology

To determine the adequacy and completeness of the criteria SEC uses to conduct capacity and security oversight, we compared the criteria with guidance issued by other financial regulators and organizations that have developed standards for auditing information systems, including the information security manual we developed for use by federal agencies.[5] We also used a list of criteria we developed based on the procedures recommended in a publication written by experts in the field of capacity planning for information systems [6] and on the findings from our prior reports or testimonies that address automation issues in the securities markets.[7] In addition, we reviewed SEC inspection work plans that the ARP staff uses to conduct on-site inspections and held discussions with SEC staff on the criteria that they use to conduct their oversight.

To determine the scope and frequency of the ARP on-site inspections, we obtained from SEC a list of on-site inspections conducted between 1995 and June 2001 of 27 SROs and electronic communication networks (ECN).[8] We reviewed a total of 11 SEC ARP inspection reports that addressed capacity planning or security-related issues, including the written reports and supporting work papers on ARP inspections of 7 SROs which included the most active exchanges as well as some of the smaller

[5]This guidance included the *Federal Financial Institution Inspection Council Information Systems Handbook, Volumes 1 and 2* (Washington, DC: 1996), which is the interagency guidance used by banking regulators; *The Capability Maturity Model: Guidelines for Improving the Software Process*, (MS: Addison Wesley Longman, 1994); the *Control Objectives for Information and Related Technology* (CobiT), Information Systems and Audit Control Foundation, CobiT Steering Committee and IT Governance Steering Committee (July 2000). In addition, we compared SEC's guidance to the *Federal Information Systems Audit Control Manual*, GAO/AIMD-12.19.6, January 1999.

[6]Vigilio A.F. Almeida, Daniel A. Menasce, and Larry W. Dowdy, *Capacity Planning and Performance Modeling: From Mainframes to Client-Server Systems*, (Upper Saddle River, NJ: Prentice Hall, 1994).

[7]These included *Securities Pricing: Actions Needed for Conversion to Decimals*, GAO/T-GGD-98-121. May 8, 1998, *Securities Pricing: Progress and Challenges in Converting to Decimals*, GAO/T-GGD-00-96, Mar. 1, 2000, and *Securities Pricing: Trading Volumes and NASD System Limitations Led to Decimal-Trading Delay*, GAO/GGD/AIMD-00-319, Sep. 20, 2000. In addition, see the list of related products at the end of this report for additional work we have done relating to information system issues in the financial markets.

[8]ECNs display and match investors' orders for stocks traded on the Nasdaq Market and the exchanges.

exchanges,[9] and just the written reports for 4 other SROs.[10] We discussed our observations of these reviews with ARP staff. To determine the scope and frequency of the independent reviews, we examined certain recent audit reports and a summary of audit reports prepared by SEC ARP staff. We also discussed the results of our assessment of these reports with SEC staff. Specifically, we reviewed copies or summaries of 37 reviews done by SRO internal audit staff for the 3 largest SROs in 2000.[11] In addition, we examined seven independent reviews of five SROs performed by external organizations that were included in the supporting work papers of the SEC inspections we reviewed.

To address how the voluntary nature of the ARP programs affects SEC oversight capabilities, we reviewed various documents prepared by the ARP staff. The documents included analyses of SRO systems, on-site inspection reports, a printout of SEC staff's database of the status of recommendations made during inspections, and oversight work plans. We conducted this work in Washington, D.C., from November 2000 to June 2001 in accordance with generally accepted government auditing standards.

SEC Uses a Wide Range of Criteria but Lacks a Consolidated Guide for Planning and Conducting Inspections

To plan and conduct inspections and other oversight activities, the ARP program uses criteria from a variety of sources that address aspects of capacity planning, security, and other information system issues. The second ARP policy statement discussed five primary areas that SEC expected that SROs would address regarding their information systems. Using these areas, the ARP staff work with SROs to develop a checklist as an initial guide for use by SEC staff in conducting their on-site inspections. This checklist was also provided to the SROs in 1991 for use as part of the independent reviews of their systems. The ARP program staff told us that

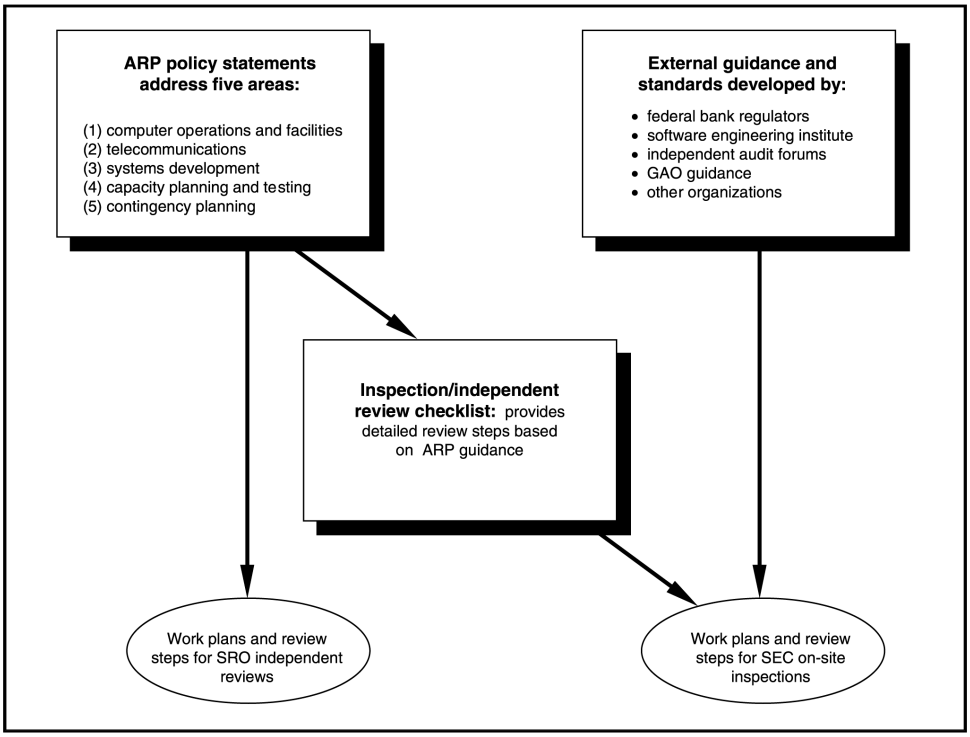
[9]The SRO inspection reports and workpapers we reviewed included those for the American Stock Exchange, the Boston Stock Exchange, the Chicago Board Options Exchange, the International Securities Exchange, the Nasdaq Market, the New York Stock Exchange, and the Options Price Reporting Authority.

[10]These reports were those for the National Securities Clearing Corporation, the Options Clearing Corporation, the New York Stock Exchange, and the Securities Industry Automation Corporation.

[11]One of the three the SROs whose internal audits we reviewed uses an external accounting firm to perform its internal audits. Of the 37 internal audit reports we reviewed, 8 were performed by an external accounting firm. SEC staff considered these reviews to be done by this SRO's internal audit staff and did not represent examples of independent reviews conducted by an external organization.

they regularly update the inspection checklist by consulting professional standards and guidance relating to information systems established by other regulatory, audit, or industry bodies. Figure 1 shows how SEC staff and the SROs use the various sets of guidance.

Figure 1: Guidance Used by ARP Program Staff



Source: GAO staff analysis.

In our review of SEC on-site inspection work papers, we observed instances in which ARP staff used the steps from this checklist to plan certain segments of work they would perform at individual SROs. SEC officials said they also expect the areas examined during inspections of SRO systems to be based on the ARP policy statements as well as on industry standards for conducting systems audits and the reviewers' professional judgment. In the work papers we reviewed, we found examples of individualized checklists that ARP staff had created that incorporated steps from the 1991 checklist and other sources for use in particular inspections of SROs. SEC staff said that checklists created for past inspections are also used to plan subsequent inspections.

ARP staff also described performing frequent Internet searches to monitor the latest information on standards and issues from various auditing and information system organizations, such as the Information Systems Audit and Control Association. At a minimum, SEC officials said that they expect their staff to perform these searches before each inspection. In their view, these additional information sources provide up-to-date, comprehensive criteria for assessing capacity planning, security, and other relevant systems issues.

ARP program staff also explained that they use their own knowledge and experience to plan the inspections and the ongoing monitoring they conduct. They said that they also added review steps to their inspections to address any current challenges facing the SROs that would affect information systems. For example, they added steps to inspections recently to address the industry's transition to decimal pricing as well as for the Year 2000 date change. They also added steps to inspections of individual SROs when new systems are being implemented or outages occur.

The Lack of a Consolidated Inspection Guide Creates the Potential for Inconsistency in Reviews

Because of continuous change in technology, SEC staff need to refer to up-to-date criteria and standards to conduct their oversight. However, they lack a consolidated guide for their staff. The 1991 inspection checklist that the ARP staff continuously updates to serve as criteria for their inspections does not address some developments in the markets and advances in information technology. For example, SEC's checklist addresses some security issues but does not include steps relating to intrusion detection. The 1991 checklist also does not address the increased risk of unauthorized access faced by SROs with information systems connected to the Internet. Although SEC officials explained that the SROs do not generally operate critical systems that use the Internet, some are using it to transmit information for less important systems, and others are considering or are already developing Internet-based systems. SEC's 1991 inspection checklist is also missing some elements relating to capacity planning. For example, the checklist did not specifically address certain issues relating to volume forecasts used in capacity planning in which some SROs have had problems. In 2000, the National Association of Securities Dealers' (NASD) transition to decimal pricing was delayed because the system NASD planned to use for decimal trading lacked sufficient capacity.[12] A review by an external organization later found that

[12]The problems experienced by NASD are discussed in our report GAO/GGD/AIMD-00-319.

NASD's volume forecasts had not adequately accounted for the increasing volatility in its trading and processing volumes. Although SEC ARP staff had identified deficiencies and made recommendations to NASD to improve its capacity planning processes, we did not find volatility of trading volumes specifically addressed in SEC's 1991 checklist or the other work plans that SEC staff prepared for the inspections we reviewed.

Because the ARP program does not have a consolidated guide for its staff, the burden of maintaining consistent quality in ARP oversight falls primarily on the most experienced ARP staff. Both SEC and other regulators frequently use comprehensive guides to ensure that the rule-compliance reviews their staff perform are consistent. For example, staff in SEC's Office of Compliance Inspections and Examinations use examination modules that consolidate the procedures for the reviews they expect their staff to perform consistently at the broker-dealers and other entities they review. However, without a similar consolidated guide, the ARP program staff must make continual efforts to consult numerous sources to supplement the areas not contained in SEC's 1991 ARP materials. Conducting quality reviews of the various SROs also requires ARP program staff to have broad knowledge of relevant issues and to be aware of how market developments could affect the systems at each SRO.

We found that the various work plans, risk analyses, and other documents prepared by the ARP program staff were generally thorough and addressed issues adequately. However, the level of detail and extent of documentation varied across staff members. Although the quality of SEC's oversight depends heavily on individual staff, the ARP program has experienced considerable staff turnover. SEC officials said that the ARP program staff has experienced turnover rates of almost 30 to 40 percent in some years. The officials said that finding replacements is always difficult, as the salaries SEC offers for people with information system skills are not competitive with the private sector. As of June 15, 2001, 4 of the 10 ARP program staff had 2 years or less of experience, including 2 staff who had just joined the program. SEC officials said that only experienced staff prepare updated workplans and lead on-site inspections. However, the lack of a consolidated written guide could lead to inconsistency in planning and conducting inspections, given the high turnover rate of ARP staff.

SEC Inspections of SROs Address Key Issues but Are Less Frequent Than SEC Staff Prefer

We found that, for the most part, SEC's on-site inspections addressed key capacity and security issues. However, resource limitations have prevented SEC from conducting inspections as frequently as their staff would prefer. During an on-site inspection, the ARP staff usually review SRO procedures, examine supporting documents, and hold discussions with SRO staff over the course of 4 to 5 days. During each inspection, ARP staff focus on the information system issues from the ARP guidance that are most relevant to the particular SRO. Although SEC staff do not conduct detailed steps to review all ARP issues during each inspection, most inspections begin with a presentation by the SRO, which the ARP staff told us covers all ARP issues. SEC staff also reported conducting some 1-day on-site inspections that focused on more limited issues. ARP staff then prepared a report that was later provided to the SROs' management.

Our review of the ARP on-site inspection reports and the supporting work papers addressing capacity and security issues indicated that, for the most part, these inspections addressed the key issues relating the SROs' procedures. We reviewed reports and supporting work papers for the most recent on-site inspections done at seven SROs and four additional inspection reports prepared between 1996 and 2000. In these documents, we found examples of detailed audit work plans that were specifically designed to address the objectives of each ARP inspection. The work papers also included documents prepared by the SROs, including their formal capacity plans and trading volume and processing load projections, which SEC staff had asked to review as part of the inspections. We also found that SEC staff had collected documents the SROs had prepared on vulnerability assessments, as well as summaries of security staff meetings. In addition, we observed instances in which SEC staff documented their reviews of the security-related steps from the review checklist.

The reports ARP staff prepared after conducting on-site inspections frequently contained numerous substantive recommendations to the SROs that addressed capacity planning, security, and other issues. For example, in an inspection done at one SRO, ARP staff made seven recommendations, including that the SRO increase the capacity of its systems, improve the security procedures for two major systems, and increase the frequency of disaster recovery testing.

Limited Staff and Other Priorities Prevent More Frequent On-site Inspections

Although SEC officials told us that the ARP program has no formal goal for the frequency of inspections, ARP staff said that they would prefer conducting on-site inspections every 12 to 18 months. However, limited staff and the need to monitor industrywide information technology initiatives have prevented them from conducting examinations this frequently. According to the information SEC provided us, SEC staff conducted 41 on-site inspections of exchange or clearing organization SROs from 1995 through June 2000.[13] During this 6-year period, ARP staff inspected most SROs once every 2 to 3 years and addressed capacity and security issues in most of these inspections. However, at least eight of these inspections lasted only 1 day. Furthermore, over this 6-year period the total number of days that ARP staff were actually on each SRO's premises was very limited. According to the data SEC provided us, we calculated that the number of days that ARP staff were on site averaged a total of 7 days at each SRO during this 6-year period, with ARP staff being on site at the least visited SRO for a total of only 4 days and at the most visited SRO for a total of 19 days.

ARP program officials explained that because of their small staff they conduct only seven or eight inspections per year. Although the ARP program had a staff of 10 as of June 15, 2001, it has had as few as 4 during some years because of generally high turnover. The staff also explained that they had spent a considerable amount of time addressing major industrywide initiatives, some of which spanned several years. These initiatives included preparations for the Year 2000 date change and the transition to trading using decimal instead of fractional prices.

SEC officials told us that they take other steps to ensure that the SROs are adequately addressing information system issues. SEC staff meet annually with the SRO officials responsible for information systems. During these day-long annual report meetings, the SRO staff provide presentations on prior and upcoming changes to their systems and on activities relating to market events that could affect system capacities, such as decimal trading and other initiatives. SEC staff told us that these meetings allow them to question the SROs and obtain copies of relevant materials. When an SRO is subject to an on-site inspection, the officials explained that the first day is usually a presentation of the SRO staff's annual report.

[13]During this time, the ARP staff also conducted 12 inspections of electronic communication networks.

Independent Reviews Mostly Conducted By SRO Internal Auditors

Although SEC originally envisioned that SRO systems would also be reviewed under the ARP program by independent external organizations, SRO internal auditors now perform the majority of these reviews. The reviews now address the key areas of ARP cyclically based upon an annual risk analysis, but we were unable to determine whether all the issues are being addressed with sufficient frequency. In addition, SEC has requested reviews by external organizations when internal audits have been insufficient or when deficiencies existed in SRO systems and procedures.

Most Independent Reviews Are Now Done By Internal Auditors Using a Risk-Based Approach

In the 1989 policy statement announcing the ARP program, SEC called for annual independent reviews of SROs that would cover capacity planning, security, and other areas.[14] SEC staff told us that at that time, SEC proposed that external organizations perform these independent reviews. However, ARP staff said that the SROs later raised concerns about the costs of implementing such reviews and the potential overlap with the SROs' own internal audit processes. ARP staff told us that they had also identified a need to modify the independent review guidance to ensure that the reviews were of sufficient depth.

As a result, SEC issued the second ARP policy statement in 1991. In addition to expanding the areas that should be reviewed at the SROs, this statement also clarified that SROs could use their internal auditors to perform the independent reviews. However, the statement noted that, if internal auditors were to be used, they should adhere to the standards set by various groups, such as the Institute of Internal Auditors and the Information Systems Audit and Control Association.[15] In addition, SEC asked that an external organization periodically assess the SRO internal auditors' independence, competency, and work performance. Since this change, the majority of the independent reviews are now done by the SROs' internal audit processes, rather than by external organizations.

SEC and the SROs have also agreed to a change in the type and frequency of the independent reviews. In December 1993, SEC and the SROs agreed that SRO staff would plan the independent reviews addressing the key areas identified in the ARP guidance, using a risk-based approach. Using this approach, the SROs' internal auditors are to determine which areas

[14]Release No. 34-27445.

[15]At that time, this organization was called the Electronic Data Processing Auditors Association.

should be examined by conducting a yearly risk analysis of the SRO's information systems. This risk analysis allows the internal audit staff to develop an audit plan that identifies the critical areas that need to be reviewed that year and less urgent issues that can be deferred until a later date. Although the SROs evaluate the risks in their systems against all of the ARP areas under this approach annually, the SEC officials explained that the SROs are not expected to review all of the key areas of the ARP guidance each year. As discussed in our Federal Information Systems Audit Control Manual (GAO/AIMD-12.19.6, January 1999), and elsewhere, such an approach is considered appropriate for reviews of this type.

Internal Audits' Coverage of ARP Areas Is Unclear

Although SEC staff said that they were generally satisfied with the quality and scope of the reviews the SROs' internal auditors had performed, we could not determine from the documents SEC staff prepared whether these reviews were addressing all the areas contained in the ARP guidance with sufficient frequency. To verify the adequacy of the SROs' efforts, ARP staff said that they also perform their own risk analyses for the SROs each year. They then are to review the SROs' risk analyses, audit plans, and past audit results to assess whether the SROs' independent reviews are addressing the ARP guidelines appropriately. When an SRO has not addressed an issue warranting attention, SEC requests a review of that area. The ARP program staff said they were also satisfied with the internal audits because many include testing of controls and compliance with procedures. In addition, the ARP staff told us that the SROs have increased the number of internal audit staff that review information system issues and that the quality of these audits has improved over time. When the ARP program first began, some of the SROs did not have internal auditors who could review information systems, and ARP staff said that their oversight efforts have resulted in increased internal audit staffing at the SROs. According to SEC staff, in the mid-1990s two major SROs had only one internal auditor specializing in information systems issues. As a result of SEC staff efforts, one of these SROs gradually increased the number of information systems auditors it employs to five.

Nevertheless, from our review of the SROs' internal audits conducted during 2000, we were unable to determine whether these reviews were addressing all of the important areas in the ARP policy statements with sufficient frequency. In one analysis we reviewed, ARP staff noted that the internal audit staff at one major SRO had not reviewed at least two of the five areas specified in the ARP policy statements since 1992 and did not state when reviews had last been conducted for the other three areas. ARP staff told us that in this case, auditors for the SRO's service vendor had reviewed at least one of the areas and information had been provided to

SEC about the other area periodically. At another SRO, the SEC staff's inspection report noted that the internal auditors had not conducted an independent review of the SRO's capacity planning process in 8 years. ARP staff told us that they had performed reviews of this area at least twice during this period. With the pace of technological change and developments in the markets, it is unclear whether this level of attention to SRO capacity planning is sufficiently frequent or appropriate.

SEC Has Called For External Reviews to Supplement Internal Audits

ARP staff told us that when SRO internal auditors do not address all the issues addressed in the ARP policy statements, the ARP staff take steps to see that they do. If their analysis indicates that internal audits have not reviewed particular issues, ARP staff said that they would consider the areas not addressed as high risk for the SROs and they would try to include them in their next on-site inspection. In some cases, ARP staff request that the SROs obtain independent reviews by an external organization when internal audits have not sufficiently addressed systems issues or because of recurring systems problems at some SROs. We found that SEC staff had recommended in at least five recent on-site inspection reports that the SROs contract with external organizations to perform reviews of SROs' capacity planning processes. For example, ARP staff requested an external review of NASD's overall capacity planning process before that market announced that the system it intended to use to transmit price quotations did not have sufficient capacity to allow it to implement decimal trading by the date SEC had set for the securities markets. In a July 2000 inspection report, the ARP program staff requested that another SRO obtain a review of all aspects of its capacity planning process because that SRO's trading volume had grown dramatically and its internal auditors had not recently addressed this process. And in 1997, after the two systems that transmit information between the stock and options markets experienced numerous delays or queues in their transmissions, ARP staff requested an external review be done of the organization that operates these systems. In March 2000, an official whose exchange relies on price data transmitted by the intermarket system for stocks told us that systems problems had caused considerable financial losses to members until its capacity was upgraded. In addition, the options exchanges and the Options Price Reporting Authority, which administers the intermarket system for options, are under an SEC order that requires them to limit the data they transmit across this system because their systems capacity is insufficient.

From a review of internal audits done at three SROs during 2000, we found that the internal audits varied in both scope and depth. We reviewed 29

internal audit reports conducted at two SROs during 2000 and a summary prepared by SEC staff of eight audits done in 2000 at another SRO that uses an external organization to conduct its internal audits. In some cases, the audits appeared to address an important ARP area thoroughly and contained substantive recommendations, including one report that identified numerous deficiencies in an SRO's contingency planning procedures. Some of the reports also indicated that the internal auditors had taken steps to test relevant controls over systems. In general, most of the internal audit reports for the three SROs that we reviewed were limited in scope, covered only one SRO system, or made minor recommendations, such as asking that one SRO obtain the most recent version of a capacity planning software program or recommending that the staff at one SRO use only one entrance to its data center. Most of the reports we reviewed addressed security or other information system issues—such as change management processes—rather than capacity planning issues.

Our review of seven reports addressing capacity and security issues that external organizations had prepared for five SROs showed that these reports generally had identified substantial deficiencies. For the most part, the SROs had obtained these reviews in response to requests by ARP staff. In one review, the external organization identified seven problems relating to an SRO's capacity planning procedures, including finding that the SRO had not collected all the data needed for its capacity planning process, identified the applications that were generating increases in processing demand, or used a standardized forecasting approach for all systems. In addition, external audit reports recommended that SROs create formal capacity planning processes and security procedures for systems that currently lack them.

The Voluntary Nature of the ARP Program Affects SEC's Capacity and Security Oversight

Because the ARP program was not established under SEC's rulemaking authority, it lacks specific rules that SEC can use to sanction SROs for not complying. Although SEC staff reported that the SROs generally comply with the ARP program, we found that in some cases SROs had not implemented ARP staff recommendations and had not always created the requested notices and reports sought under ARP. When establishing the ARP program, SEC left open the possibility of making the program mandatory but did not establish criteria to assess the level of cooperation under the voluntary program.

ARP Program Lacks Specific Rules

The policy statements issued when SEC began the ARP program established voluntary guidelines for the SROs to follow regarding the capacity and security of their information systems. These guidelines called

for the SROs to have independent reviews performed on their systems and to make various reports and notices to SEC. However, the program was not established under SEC's rule making process. SEC officials explained that the view of the staff at the time was that any specific standards relating to information systems included in such a rule could become obsolete in a short period of time. SEC staff would then be required to seek amendments to the rule, which would also likely take considerable time and effort to complete. In their view, voluntary guidelines afford SEC staff greater flexibility. However, by issuing only voluntary guidelines, SEC staff have no specific rules to require SROs to implement key ARP recommendations or create the reports or notices called for in the policy statements and cannot sanction SROs under the ARP program for failing to do so. SEC officials said that they believed they could bring an official action against SROs whose failure to follow ARP was serious enough to represent a violation of the general requirement that exchanges maintain the ability to operate. They said, however, that SEC rarely uses such authority.

Some Significant ARP Program Recommendations Not Being Implemented and Concerns Not Addressed

ARP staff acknowledged that SROs have not addressed several significant capacity and security recommendations or concerns raised in ARP inspections. For example, we previously reported that in 1996, ARP staff recommended that NASD establish capacity alternatives to meet unexpected system demand.[16] However, NASD has continued to experience capacity-related problems with several of its systems, disrupting the markets. For example, insufficient capacity in NASD's price-quotation system delayed the start of decimal trading by all securities markets for 3 months and prevented NASD from fully trading in decimals for an additional 7 months. As a result, investor benefits from the reduced spreads that have resulted from decimal trading on the Nasdaq market were delayed by an additional 10 months. In addition, NASD has experienced capacity-related delays in a system that transmits orders to buy or sell shares in response to displayed price quotations. Officials from a major ECN told us in 2000 that they have experienced losses of up to $1.5 million a day because they are obligated to honor orders that arrive late through this system for shares that have already been sold to their own customers. Honoring these delayed orders can produce losses because the ECN sometimes has to execute new orders at disadvantageous prices if the price of the security has changed since the original transaction. Finally, NASD experienced trading disruptions on

[16] GAO/GGD/AIMD-00-319.

June 28, 2001 because the number of market participants given access to one of its systems exceeded the number of market participants that system had been programmed to handle.[17] NASD officials said that the system was set up to handle about 90 users at once; however, by that date the number of users exceeded this figure by about 30 percent, and the system software had not been modified to account for this growth.

Other important ARP recommendations and concerns that were not being implemented or addressed dealt with SROs' security procedures, including their contingency plans for addressing physical threats or damage. In 2000, ARP staff recommended that one SRO develop and publish security policy and procedures and enforce them through a central authority, in accordance with basic industry standards. The SRO disagreed with the ARP recommendations, preferring to leave its security procedures decentralized. Another ARP staff recommendation that one SRO develop a recovery plan for trading facilities used for two of its most actively traded securities has been outstanding since at least 1995. Although this SRO has discussed various alternatives during this period for continuing operations in the event that its trading floor becomes unavailable, as of July 2001, its staff had still not implemented an alternative approach.

In addition, although ARP program staff considered the lack of backup facilities to be a major deficiency, ARP program staff have recommended in other cases that SROs perform studies rather than take actions to resolve the deficiencies. In at least three cases, ARP staff recommended that SROs study the feasibility of establishing such facilities to avoid potentially lengthy shutdowns should their trading locations became unusable. One SRO disagreed with the recommendation, citing the costliness of maintaining such facilities, and the other SROs performed or are performing the studies. However, none has taken steps that fully address the ARP staff concerns that major physical damage to the trading floors could render these SROs unable to operate for an extended period.

SROs Do Not Consistently Provide Information

Although the ARP program calls for the SROs to create certain reports to SEC when outages or other disruptions occur that affects their systems, these reports were not always being made. As stated in the second ARP policy statement, the SROs are to report immediately to SEC systems

[17]Specifically, this limitation only affects this system's ability to resume trading in a stock after such trading has been halted for impending news or other reasons.

outages that are expected to last longer than 30 minutes and report shorter outages after systems have been repaired. In addition, the second ARP statement recommended that SROs provide SEC with notices of significant system modifications. According to ARP staff, approximately 100 system outages were reported in fiscal year 2000, and for more than half of these, SEC officials said that they asked the SROs to provide analyses or other documentation of the event. SEC staff said that most SROs provide notices of outages or system modifications, but that some important outages or changes have not been reported. According to the findings from an SEC on-site inspection, one SRO lacked procedures for ensuring that notices of system modifications would be created and provided to SEC. In response, this SRO agreed to implement appropriate procedures. Another ARP inspection found that one SRO had failed to report at least six system outages during 2000. If SROs were required by SEC rule to provide SEC with notifications of significant changes to their automated systems, then the failure to have procedures in place for ensuring that notices of systems modifications are provided to SEC would likely demonstrate a weakness in the SRO's internal controls. If the deficiency was severe enough, SEC could initiate an enforcement proceeding.

In some cases, SEC staff became aware of anticipated SRO system changes from press or trade publications. For example, ARP staff learned of the proposed 1998 sale of one SRO's options trading operations to another in a newspaper report. Although some of these instances involved proposed system changes that had not been finalized by the SROs, not knowing the most current configuration for the SROs systems could make planning inspections and other oversight activities more difficult for SEC staff.

SEC Has Not Developed Formal Criteria and Assessed SRO Cooperation With the ARP Program

SEC stated in its initial ARP release that it would consider making the ARP program mandatory if SROs did not cooperate fully. However, SEC has yet to develop formal criteria and perform an assessment of SRO cooperation. In 1998, SEC's Office of Inspector General reported that SEC had not indicated how it would assess compliance with the ARP program.[18] Because of the increased importance of information technology to the functioning of the securities markets, the Inspector General's report recommended that the agency consider making the ARP program

[18]SEC Office of Inspector General, *Oversight of SRO Automation*, (May 1998).

mandatory. In response to this recommendation, ARP program staff said that they had considered the issue and determined that ARP should remain voluntary. SEC staff said that a substantial lack of cooperation with ARP would be inconsistent with an SRO's general obligations, but they were satisfied with the extent to which SROs cooperate.

Conclusions

The use of information technology is pervasive in the securities industry, and the quality of the SROs' systems is vital to the functioning of the markets. Based on our review, the ARP program provides SEC staff with some assurance that SROs are addressing capacity planning, security, and other information system issues. In addition, the ARP staff performed comprehensive and in-depth inspections of SRO systems, and were actively involved in the industry's recent completion of efforts to ready systems for the Year 2000 date change and the transition to decimal trading.

Various aspects of the ARP program highlight areas in which SEC's oversight could be strengthened to better assure that the SROs manage their critical information systems sufficiently to prevent major disruptions in the markets. Although SEC staff consulted an extensive array of standards and guidance to ensure that their oversight addresses relevant issues, the lack of a consolidated inspection guide for their staff means that the consistency and quality of SEC's oversight is heavily dependent on the efforts of the individual ARP staff. A consolidated inspection guide could take the existing five ARP areas and provide additional topics that the SEC staff find are most relevant given the current state of technology in the markets. Rather than duplicating external guidance that SEC staff already use, a consolidated inspection guide could enumerate these other sources and incorporate, by reference, the specific areas that the SEC staff have found relevant to their work. Having a consolidated inspection guide for its staff would better ensure that SEC's ARP program oversight is conducted thoroughly and consistently across its staff. This is particularly important because the program has high turnover that results in significant portions of its staff having little or no experience.

SEC's ability to oversee information system issues is also hampered by the limited resources available to the ARP program, which constrains its staffs' ability to inspect the SROs more frequently. SEC now relies largely on the SROs' own internal auditors to review systems in detail instead of more routinely using external organizations as an independent check on the activities of the SROs, as was originally envisioned under the ARP program. In cases in which the internal audits had not sufficiently

addressed issues or when SROs had deficiencies in their information system procedures, SEC staff have called for SROs to obtain external reviews of their systems.

When combined with the reliance on internal audits, the ARP program's voluntary nature raised concerns that SEC's oversight efforts are not as effective as they could be. SRO cooperation in implementing significant SEC recommendations has been uneven. The SROs' unwillingness to make recommended improvements may have adversely affected the markets, for example, when capacity problems at one market delayed full implementation of decimal trading for all securities markets. Because some SROs have not addressed ARP staff concerns over the lack of backup trading facilities, securities trading in the United States could be severely limited if a terrorist attack or a natural disaster damaged one of these exchange's trading floor. When SROs are not implementing significant recommendations or taking steps to remedy identified capacity and security weaknesses, SEC's Chairman and Commissioners could focus additional SRO attention on the need to take actions to improve their systems.

SEC's ARP policy statements left open the possibility of having a rule-based program if compliance was not adequate. Developing formal criteria and performing an assessment of SROs' compliance with the ARP program would allow SEC to determine whether a rule-based program would be warranted. Such an assessment also could weigh the advantages and disadvantages of the current voluntary program and whether it provides SEC with sufficient authority to optimally ensure that SROs' systems are sound. Criteria and an assessment could allow SEC to determine whether failure to implement recommendations risked material disruption in the markets. Making the ARP program mandatory could give SEC the authority it needs to better assure that SROs take cost-effective steps to improve their systems and procedures and reduce the risk of systems-related problems disrupting the markets. On the other hand, if the program were to be made mandatory, SEC would need to build adequate flexibility into the governing rule to deal with technological change.

Recommendations

Because of the importance of the proper functioning of the SROs' information systems, we recommend that the Acting Chairman, SEC, take the following actions:

- ensure that the ARP program develops a consolidated inspection guide for the ARP staff that is updated on a periodic basis,

- ensure that significant ARP program recommendations and concerns that have not been addressed by the SROs are brought to the attention of the Chairman and the Commissioners, and
- develop formal criteria for assessing the SROs' cooperation with the ARP program and perform an assessment to determine whether the voluntary status of the ARP program is appropriate.

Agency Comments

We obtained comments on a draft of this report from SEC, which are presented in appendix I. In its letter, SEC commented that the draft report was based on an inaccurate view of the ARP program, and that it did not reflect the development of the program since SEC issued its two ARP policy statements in 1989 and 1991. SEC provided an extensive discussion of the ARP program's evolution over time. In response, we have made language changes where appropriate and believe that our report fairly presents the evolution of the ARP program over time. However, although the ARP program has achieved some important goals, we think that it could be more efficient and effective if our recommendations were adopted.

SEC generally disagreed with our recommendations, noting that activities they already perform satisfy the intent of the recommendations. Specifically, SEC did not see a need to develop a consolidated inspection guide because it would quickly become outdated and the ARP staff's approach to developing work plans for individual inspection results in oversight that addresses key capacity and security issues. The ARP staff's approach has, to date, generally resulted in oversight that addresses key issues. However, given the high staff turnover and the relative inexperience of many staff, we are recommending that ARP develop a guide that will assure continued consistency. Moreover, we believe that such standard guides are a good business practice and a sound internal control. The type of guide that we recommend would also require minimal effort to update because it would largely incorporate by reference standards and criteria developed by other organizations, which would likely be updated by those organizations regularly.

With respect to our recommendation that SEC develop a process to bring significant unimplemented ARP recommendations and outstanding concerns to the attention of the Chairman and the Commissioners, SEC commented it had a process that satisfied the recommendation. In its letter, SEC noted that it already reviews the status of all ARP recommendations. SEC also stated that where an SRO's response to ARP recommendations is unsatisfactory, SEC has a procedure to bring the

matter to the attention of the Division Director and, if necessary, to the Chairman and Commissioners. SEC commented that, based on discussions with us, the staff was enhancing its process for reviewing the status of ARP recommendations and updating the recommendations database. We note, however, that according to SEC officials, no unimplemented ARP recommendations or concerns have been escalated beyond the Division Director level. We believe that some significant unimplemented ARP recommendations and concerns regarding capacity and security weaknesses at the exchanges and clearing organizations warrant attention at the highest levels of the Commission. Involvement at this level would increase the likelihood that SROs would take meaningful action in response to such recommendations and concerns. Therefore, we reaffirm our recommendation.

SEC also disagreed with our recommendation that it develop formal criteria for assessing SRO compliance with the ARP program. SEC commented that the risk assessment process the ARP program staff conducts annually for each SRO represents their assessment of the SRO's compliance with the ARP policy statements and that when SROs do not implement ARP recommendations or remedy concerns, they call for additional inspections and reviews. Although we agree that the ARP staff's efforts have resulted in some improvements in the SROs' information systems, we remain concerned that some recommendations that SROs have not fully addressed pose a greater risk of further market disruptions. Moreover, seeking to address noncompliance with the ARP program by performing additional inspections would likely result in ARP staff identifying many of the same discrepancies over time. For example, ARP staff found capacity-related problems over several years at NASD and have had long-standing concerns about contingency planning alternatives at some SROs.

SEC's risk assessment process, although allowing it to adequately plan its oversight, does not constitute or supplant the type of assessment of overall program compliance that we recommend. Instead, by developing formal criteria and assessing the overall level of compliance with the ARP program, SEC would have a sound basis for evaluating the nature of the program. Even if no change in its status were made after such an assessment, periodically reapplying the criteria would allow SEC to assess the pattern of compliance by SROs over time to ensure that the program's status is not hampering the effectiveness of SEC's oversight of the SRO information systems that are critical for continued market functioning.

SEC also commented that neither GAO nor SEC itself has any basis to believe that the voluntary nature of the program is problematic. However, we did identify various instances in which SROs were not addressing recommendations or taking actions in response to ARP staff concerns or were not making the reports that SEC has requested. Furthermore, we are not recommending that SEC make the ARP program mandatory, but instead have recommended that SEC develop formal criteria to assess whether the program is working as it is currently structured.

SEC also provided technical comments that we incorporated as appropriate, including refining our presentation of the extent to which ARP program recommendations have not been implemented. In addition, we revised the language of the report and our recommendation to clarify that the SEC Chairman and Commissioners should be advised when significant recommendations to SROs are not implemented or SRO actions do not address ARP staff concerns.

As agreed with you, unless you publicly release its contents earlier, we plan no further distribution of this letter until 30 days from its issuance date. At that time, we will send copies to the Chairman and Ranking Minority Member, Senate Committee on Banking, Housing, and Urban Affairs; the Chairman and Ranking Minority Member, House Committee on Financial Services; the Chairman, House Committee on Energy and Commerce; and the Acting Chairman, SEC. We will also make copies available to others upon request.

If you have any further questions, please call me at (202) 512-8678 or Cody J. Goebel, Assistant Director, at (202) 512-7329.

Sincerely yours,

Davi M. D'Agostino, Director
Financial Markets and
Community Investment

Appendix I: Comments From the Securities and Exchange Commission

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

DIVISION OF
MARKET REGULATION

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

July 18, 2001

Ms. Davi M. D'Agostino
Director, Financial Markets
and Community Investment
United States General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Ms. D'Agostino:

This letter responds to the request from Cody Goebel, Assistant Director, Financial Markets and Community Investment, on July 2, 2001 to review and comment on the draft Report entitled Opportunities Exist to Strengthen SEC's Oversight of Capacity and Security, GAO/GAO-01-863.

Thank you for the opportunity to comment on the draft GAO Report. The GAO Report recommends that the SEC take the following actions: (1) ensure that the SEC's Automation Review Policy (ARP) program develops a consolidated inspection guide for the ARP staff that is updated on a periodic basis; (2) develop a process to bring significant unimplemented ARP program recommendations to the attention of the Chairman and the Commissioners; and (3) develop formal criteria for assessing SRO compliance with the ARP program and perform such an assessment to determine whether the voluntary status is still appropriate for the goal of the ARP program.

The Terms of Work that the GAO provided to Congressman Dingell on June 11, 2001, focused on "SEC oversight of capacity and security issues at the various self-regulatory organizations (SRO) and how capacity issues are coordinated among these organizations." The draft Report commends the Commission's oversight efforts in these important areas. The draft Report compares the criteria that the SEC provided to the SROs on information security and capacity planning with guidance issued by a variety of other organizations, and concluded that our on-site inspections "addressed key capacity and security issues" (p. 11), "overall, SEC's inspections addressed the key areas of ARP guidance" (p. 2), and the ARP "workplans, risk analyses, and other documents prepared by the ARP program staff were generally thorough and addressed issues adequately" (p. 10). The draft Report also finds that our inspection reports "contain numerous substantive recommendations to the SROs that addressed capacity planning, security and other issues" (p. 12), and our risk assessment approach is "considered appropriate for reviews of this type by [the GAO's] own information systems guidance" (p. 14). We appreciate the GAO's recognition that the SEC's oversight program appropriately addresses key issues related to capacity and security at SROs. We are proud of the efficient and effective manner in which the ARP staff oversees these important issues at the SROs.

See comment 1.

In the short time period that we have had to comment on the draft Report, it is difficult to address specifically the remainder of the Report, which in our view departs substantially from the Terms of Work and contains many vague and unsubstantiated statements regarding the overall operation of the ARP program. In particular, we believe that the draft Report does not reflect the development of the program since the Commission issued the 1989 and 1991 ARP policy statements, and, in particular, the development of a risk assessment approach to ARP implementation. The Report overlooks the important distinction between a program that is tasked with overseeing information technology, a field in which no single set of standards exists, and other programs that are based on assessing compliance with rules that lend themselves to bright-line tests. However, the draft Report implicitly acknowledges the unique nature of oversight in the IT area because it does not identify any single authoritative source for standards in IT security and capacity planning.[1]

Because of the limited response time available, we do not address each deficiency in the draft Report.[2] Because we believe that the draft Report is based on an inaccurate view of the ARP program and does not reflect the current operation and effectiveness of the program, we provide a description of the ARP program as it has evolved over the past twelve years. We also comment on the GAO's three specific recommendations.

The SEC's Automation Review Program

The First Phase of ARP

The Commission established its automation review program (ARP) after the October 1987 market break and the October 1989 market decline by issuing two policy statements regarding the use of technology in the securities markets.[3] In the first statement, ARP I, which was issued in November 1989, the Commission called for the SROs to establish, on a voluntary basis, comprehensive planning, testing, and assessment programs to determine systems capacity and vulnerability, and obtain annual independent assessments of systems to determine whether they can perform adequately. The second statement, ARP II, was issued in 1991 and set forth guidance concerning the nature of the independent reviews of the general controls[4] for the SROs' electronic data processing

---

[1] Instead, in conducting its audit of the SEC's ARP oversight program, GAO examiners used the same collection of guidelines that SEC ARP staff use (and which we identified to the GAO at the outset of this audit) in conducting ARP inspections -- guidance issued by other financial regulators and professional organizations for auditing information systems on security and capacity planning. See GAO draft Report, p. 6 n.5.

[2] We address a few of the draft Report's inaccuracies in the attached Addendum of technical comments.

[3] Securities Exchange Act Release Nos. 27445 (November 16, 1989) [54 Fed. Reg. 48703] (ARP I) and 29185 (May 9, 1991) [56 Fed. Reg. 22490] (ARP II).

[4] General information controls are those controls within an organization's information systems environment that significantly influence the effectiveness of application controls. General controls are designed to ensure that information processing takes place in a reasonably controlled and consistent environment. As

(EDP) systems, which the SROs are encouraged to obtain in ARP I, and called for periodic independent reviews of these controls, with the resulting report presented to both SRO management and the Commission.[5]

Under the independent review process outlined in ARP II, the general controls reviews were initially based upon a checklist set of questions used to examine five areas where general systems controls could be weak or missing: 1) computer operations; 2) telecommunications/data security; 3) systems development methodology; 4) capacity planning and testing; and 5) contingency planning.[6] The Commission expected the ARP reviews to be conducted pursuant to industry standards regarding methodology, independence, work performance, and documentation.[7] To assist the SROs in reducing the costs involved in ARP reviews, the Commission suggested that each SRO choose whether to employ its internal audit department, if one existed, or an outside accounting or consulting firm experienced in EDP assessments to conduct the internal review of the SROs' general system controls.[8]

In addition to ARP I and ARP II, in 1992 the Commission created an office within the Division of Market Regulation to oversee the SROs' implementation of the ARP recommendations. The ARP staff was tasked with overseeing the SROs' reviews of their EDP operations. In this role, the staff would not conduct a direct examination of the SRO's EDP systems. Rather, ARP contemplated that the SROs would make available to the Commission the independent reviewer's written conclusions and recommendations to SRO management and information regarding the internal reviewer's independence (if the review is conducted by the SRO's internal audit group). The Division's ARP group conducts on-site inspections of the SRO's ARP review by examining the materials produced during the review and conducting interviews of responsible personnel at the SRO. The result of the inspection is a report by the Division to SRO management providing the Division's assessment of the SRO's performance under the ARP guidelines and making recommendations for improving SRO performance in these areas.

---

such, these controls, including those related to computer operations, systems development, data security, and telecommunications, have an impact on the effectiveness of all controls and processing functions that involve the use of information systems. See the Institute on Internal Auditors Research Foundation "Systems Auditability and Control" Module 2, at 2-13 (1991).

[5] In ARP II, the Commission also presented the SROs with guidelines for additional means of providing the Commission with information regarding automation developments and concerns, especially new system developments or enhancements and system outages. Specifically, ARP II called for: 1) annual reports through which SRO technical staff would describe for Division staff the current automated system operations and planned system changes; 2) SRO notification to the Division of significant changes to automated systems; and 3) notification of significant interruptions of service in SRO automated trading systems. ARP II, 56 Fed. Reg. at 22493-22494.

[6] The initial checklist could be that produced by the joint efforts of the Commission staff and the SROs (the "1991 SEC/SRO checklist") or a similar document.

[7] ARP II, 56 Fed. Reg. at 22492.

[8] ARP II, 56 Fed. Reg. at 22492 n.9.

By the end of 1993, Division staff had completed a full-cycle of ARP inspections of the independent reviews of automation controls at the SROs. In this first cycle – or First Phase of ARP implementation – the SROs performed general controls reviews of automated trading and information dissemination systems that had never been done before in a systematic manner. Division staff thereafter inspected all of the SROs to determine the effectiveness of general controls reviews and to assess whether SRO management adequately responded to auditor recommendations. As reported to the Commission, the Division generally was satisfied that each SRO performed an adequate baseline review and had begun to address weaknesses in EDP system controls. The First Phase oversight reviews of the SROs conducted by the ARP staff acted as a significant force in stimulating the SROs to strengthen the independence of the audit operation, and to upgrade their systems technology and the system controls in place.

Adoption of the Risk Assessment Approach

ARP I and II did not establish the frequency and depth of reviews and did not specifically call for or establish a methodology for reviews of controls that protect specific applications.[9] However, generally accepted EDP auditing procedures at the time suggested a periodic review of general controls and also suggested guidelines regarding the need for reviews of application controls.[10] With those guidelines in mind and prompted by requests for guidance by the SROs, the Division addressed these outstanding issues in a series of meetings with the SROs during 1993 to identify methods to implement the ARP policy statements in a cost-effective manner while maintaining the necessary quality of reviews. During these meetings, the SROs expressed the view that under an SRO's typical audit planning process, it may not be feasible to establish a uniform cycle of EDP reviews, e.g., every two to three years for every SRO, irrespective of each SRO's particular circumstances.

As a result of these consultations, the Division developed – and the Commission endorsed – a new approach to the planning, scope, and implementation of automation reviews at the SROs, intended to enhance the effectiveness of the ARP program and define the cycle of ARP inspections. According to this approach, each year, the SRO's internal auditor performs a risk assessment of areas subject to audit to identify which areas pose the greatest degree of risk, and which would be selected for audit. By incorporating ARP review concepts into the SROs' pre-existing risk assessment approach

[9] Application controls are specific to the flow of transactions (i.e., data) for a particular system or function, are designed to ensure authorized, accurate, and complete processing of a transaction from input, through processing, to the output of information. Application controls are designed to prevent, detect, or correct errors and irregularities as transactions flow through the system. See Institute of Internal Auditors Research Foundation "Systems Auditability and Control," Module 2, at 2-7 (1991).

[10] EDP audit guidance suggests that the organization's internal audit function include periodic review of all aspects of the information services department's activities. See "Controls in a Computer Environment: Objectives, Guidelines and Audit Procedures," at I-1-15, by the Electronic Data Processing Auditors Foundation (1992).

to audit work, the entire process could be made more efficient and effective. Under this approach, the exchanges annually perform a risk assessment of EDP operations, including significant trading and information dissemination applications. The auditors perform audits of any systems or applications that ranked high in risk.[11] The SRO internal auditors furnish the Division with its audit universe, risk assessment, audit plans, and audit reports. By building on sound business processes displayed by the SROs, we expected that the risk assessment approach would lower ARP review costs, and would expand the scope and frequency of EDP reviews at the SROs. Since 1993, the SROs have followed the risk assessment approach with good results.

Using the results of the SRO risk assessment process and other pertinent information, the Division annually conducts its own risk analysis to determine if an ARP inspection is needed. To accomplish this, the Division uses industry-accepted auditing principles to provide reasonable assurance that the SRO has controls in place that are adequate to meet the goals established by the SRO's management. When the Division determines to perform an ARP inspection of a SRO, the inspection involves a review of internal and/or external auditor work, as well as direct examination of targeted aspects of EDP operations, which provides information regarding whether controls over EDP operations are working as designed.[12] Based on its annual risk assessment and on-site inspections, Division staff may determine that an SRO has gaps or weaknesses in its ARP performance, which results in a Division inspection report that recommends that the SRO take steps to improve its performance, or obtain an independent assessment of specific ARP areas of weakness.

In summary, the SEC has developed a reasonable and cost-effective program that provides reasonable assurance that the SROs' automated systems are being rigorously developed and managed with respect to capacity, security, systems development methodology, telecommunications, and contingency planning. The Commission's risk assessment approach, which replaced the general controls reviews that the SROs and Division staff conducted in the First Phase of ARP implementation, provides information to decision makers at the SROs so that they can understand factors that negatively influence operations and make informed judgments concerning the actions needed to reduce the risk. The voluntary nature of the program and use of up-to-date, work plans tailored to each SRO's systems environment permits the SEC to respond flexibly to

[11] The risk assessment approach applies whether an SRO uses an internal or external auditor. Pursuant to the risk assessment approach, SROs conduct EDP audits, which involve detailed examinations and testing of the systems or applications or supporting IT infrastructure. These audits provide the Division with more in-depth information than the general controls reviews of the First Phase of ARP implementation.

[12] The draft Report states that eight of the fifty-three inspections that we conducted between 1995 and 2000 lasted only a day and that the length of time ARP staff spent on-site ranged between four days and nineteen days (p. 12). Based upon the Division's annual risk assessments of the SROs, we determine which SROs should be inspected and the areas that should be examined, which in turn establish the duration of the inspection.

changes in SRO technology and business practices. Through this program, the SEC has been successful in working with the SROs to improve controls over their automated systems, to monitor the safety and soundness of the nation's securities markets in a cost-effective manner and reduce – albeit not entirely eliminate – the risk of a systems-related market disruption.

Response to Specific GAO Recommendations

1. The GAO recommends that the Commission take action to ensure that the ARP program develops a consolidated inspection guide for the ARP staff that is updated on a periodic basis.

In the face of constantly changing technology and information processing environments that significantly differ among the SROs, the Division has determined that a single, generic, static consolidated inspection guide would be outdated as quickly as it is generated and would not be a useful tool to use for all SROs' system environments. Instead, the Division's approach, which has worked quite well, uses very functional, up-to-date inspection guides, or work plans, that experienced Division staff tailor to current industry guidelines and technological innovations as well as to the particular SRO's systems.

In preparation for each on-site inspection, the desk officer assigned to the SRO conducts a professional literature search and prepares the work plan. A senior computer specialist carefully reviews the work plan for consistency and appropriate coverage of the ARP areas. Only experienced staff are assigned lead responsibility for ARP inspections.[13]

See comment 1.

The draft Report assumes that the 1991 SEC/SRO checklist is the principal tool used by Division staff in conducting inspections. This is not correct.[14] The 1991 checklist was developed to provide guidance to the SROs in the First Phase of ARP implementation, prior to 1993. Since 1993, Division staff have revised this checklist numerous times, and have continually supplemented it with material from a variety of up-to-date professional sources.[15] The revised checklist, prior work plans and current professional sources provide a comprehensive "menu" from which the appropriate elements are selected to assemble a work plan tailored to the SRO to be inspected. Prior to each inspection, we identify for the SRO the issues we intend to address. The draft Report comments favorably on the effectiveness of this procedure by stating that our on-site inspections "addressed key capacity and security issues" (p.11), and the ARP

[13] Newer staff typically serve in an apprentice role to a more experienced ARP staff person for at least six months to a year. After this "apprenticeship," the Division assigns them lead, or desk officer, responsibilities for one or more SROs.
[14] We cannot represent whether SROs may still use the 1991 checklist.
[15] See n.1 above.

"workplans, risk analyses, and other documents prepared by the ARP program staff were generally thorough and addressed issues adequately" (p. 10). Accordingly, we believe that our methodology satisfies what we understand to be the objective of the draft Report's recommendation.

2. The GAO recommends that the Commission take action to develop a process to bring significant unimplemented ARP program recommendations to the attention of the Chairman and the Commissioners.

The Division currently has a process for reviewing the status of all ARP recommendations. In connection with on-site inspections, Division staff review the outstanding recommendations from prior ARP inspections (which are recorded in a recommendations database). The Division's inspection includes an assessment of the status of implementation of the outstanding ARP recommendations. The SRO's progress in responding to these recommendations is included in the report of the inspection. In situations where an SRO's response to the recommendations is unsatisfactory, we implement an escalation procedure to the Division Director and, if necessary, to the Chairman and/or the Commission. We believe this escalation process satisfies the GAO's recommendation.

Based upon our discussions with GAO staff, however, we are undertaking to enhance our process for reviewing the status of ARP recommendations as part of our annual risk assessment of each SRO. We have also identified a need to improve the updating of our recommendations database. For example, we are in the process of developing additional staff guidance for closing recommendations where changes to SROs' systems environments make old recommendations moot.

3. The GAO recommends that the Commission take action to develop formal criteria for assessing SRO compliance with the ARP program and perform such an assessment to determine whether the voluntary status is still appropriate for the goal of the ARP program.

The Division already has in place a formal process for assessing SRO compliance with the ARP program. As described above, in 1993, the Commission approved a risk assessment-based approach to overseeing ARP performance. Under this approach, the Division seeks to reduce the risk that SRO systems controls may be inadequate and lead to a market disruption. The Commission has never represented that it will – or that it has the capacity to – certify that SRO systems' controls are adequate to prevent a market disruption. Rather, as expressed by the GAO, risk assessments "are a means of providing decisionmakers with information needed to understand factors that can negatively influence operations and outcomes and make informed judgments concerning the extent

of actions needed to reduce risk."[16] The risk assessments of the SROs' systems conducted by the SROs and by Division staff serve this purpose in an effective manner. SRO compliance with ARP is properly measured by the risk assessment process.

As described above, the risk assessment approach provides a two-stage assessment mechanism for determining whether SROs are implementing ARP, by incorporating an annual risk assessment performed at each SRO as well as an annual risk assessment conducted by Division staff. In addition, where necessary and appropriate, Division staff recommends that SROs obtain an outside assessment of a focused aspect (such as capacity planning) of the SRO's ARP compliance, which serves as a third assessment mechanism. The Division carefully monitors SROs' responses and implementation of any Division and consultant recommendations.

As part of the ARP inspection process, the Division typically makes recommendations to the SROs related to perceived weaknesses or deficiencies in the SRO's controls over its information processing systems. Through these recommendations, we provide information to senior management at the SROs regarding potential risks in their systems controls so that they can make informed decisions. We examine the manner in which the SROs addressed our recommendations during our annual risk assessment. In cases of less than complete agreement by the SRO to implement our recommended changes, we may determine to inspect the SRO more frequently, in order to more closely oversee systems controls. We believe that this is the appropriate approach for assessing compliance with ARP and has proven effective in reducing the risk that SROs' systems controls are not adequate to prevent market disruptions.

Neither the GAO nor the Commission has a basis to believe that the voluntary nature of the ARP program is problematic.[17] The draft Report's implication that the success of the ARP program should be measured against the number of open ARP recommendations reflected in our database overlooks the fundamental aspects of the

[16] "Information Security Risk Assessment – Practices of Leading Organizations," GAO/AIMD-00-33, Sept. 1999, at 6. See "Federal Information Systems Audit Control Manual," GAO/AIMD-12.19.6, Jan. 1999, chapters 2 and 3.1 ("FISCAM").

[17] The draft Report suggests that the failure of SROs to implement certain ARP recommendations may have led to substantial systems problems at Nasdaq and the New York Stock Exchange. Regarding Nasdaq, we identified a concern and recommended that Nasdaq obtain an independent assessment of its capacity planning well before Nasdaq announced that its systems would not be ready for decimalization by summer 2000. Nasdaq agreed to this recommendation and was in the process of hiring the consultant when Nasdaq determined, based on internal testing, that its systems would not be able to handle the projected volume growth associated with decimals as well as organic growth projections. Ultimately, no systems problems occurred in the transition to decimals. Regarding the NYSE, the Division is in the process of reviewing the June 8, 2001 systems outage.

Commission's risk assessment approach to monitoring ARP compliance.[18] As discussed above, the risk assessment approach provides decision makers at the SROs with information – including recommendations by internal and external audit groups and by Commission staff – that identifies potential factors that may negatively influence systems performance. Using this information, decision makers make informed judgments, which may include implementing a SEC staff recommendation over several years, disagreeing with the critical nature of the recommendation, or hiring an independent consultant to provide a third opinion about the systems risks and alternative ways to mitigate the risks. Through the risk assessment process, the Division monitors SRO compliance with the ARP program.

As the Commission stated in ARP II, we continue to assess whether rulemaking is appropriate in this area. Based upon the results of the ARP program to-date, and after weighing the considerations relating to the appropriateness of rulemaking in this area, we have determined that it is appropriate to continue the ARP program on a voluntary basis.

* * *

Thank you again for the consideration that you and your staff have shown to our staff and the opportunity to comment on this draft Report. Please contact us if it would be useful for us to elaborate on the discussion in this letter.

Sincerely,

Annette L. Nazareth
Director

Attachment

[18] We have recently examined and updated our recommendations database, and found that we made 128 recommendations (this is an increase over the preliminary total of 105 that we provided earlier to the GAO) between February 1995 and December 2000. Of the 55 "open" recommendations identified by the GAO, we have determined that 36 should be closed because our database was outdated. Of the remaining 19 open recommendations, most (15) were made in 2000. The SROs have informed us that they are in the process of addressing these 15 recommendations.

The following are GAO's comments on the Securities and Exchange Commission's letter dated July 18, 2001.

GAO's Comments

1. SEC's letter states that our report overlooks the important distinction between a program that is tasked with overseeing information technology, in which no single set of standards exists, and other programs based on assessing compliance with rules that lend themselves to bright-line tests. However, we believe that our report acknowledges the evolving nature of information systems and the lack of one source for standards, but also offers suggestions to improve SEC's oversight of this area. For this reason, we recommended that SEC create a consolidated guide for its staff of the most up-to-date and authoritative sources for criteria for planning their oversight activities. We also believe that rules can be drafted to allow sufficient flexibility for information technology advances. Furthermore, many examination programs assess compliance using professional judgment against criteria even when bright lines do not exist.

2. SEC's letter states that our report assumes that its 1991 checklist is the principal tool used by SEC staff to conduct inspections. However, our report describes the process SEC staff uses to plan inspections, including drawing on external criteria and using work plans and checklists from more recent inspections. However, we did observe instances in which the staff continued to use the 1991 checklist, but had to supplement the areas that it does not address with all the other sources.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Davi M. D'Agostino, (202) 512-8678

Cody J. Goebel, (202) 512-7329

Acknowledgments

In addition to those named above, Ronald W. Beers, Emily R. Chalmers, Heather T. Dignan, William Lew, and Jean-Paul Reveyoso made key contributions to this report.

Related GAO Products

Securities Pricing: Trading Volumes and NASD System Limitations Led to Decimal-Trading Delay, GAO/GGD/AIMD-00-319, Sep. 20, 2000.

Securities Pricing: Progress and Challenges in Coverting to Decimals, GAO/T-GGD-00-96, Mar. 1, 2000.

Securities Pricing: Actions Needed for Conversion to Decimals, GAO/T-GGD-98-121, May 8, 1998.

Financial Markets: Stronger System Controls and Oversight Needed to Prevent NASD Computer Outages, GAO/AIMD-95-22, Dec. 21, 1994.

Financial Markets: Computer Security Controls at Five Stock Exchanges Need Strengthening, GAO/IMTEC-91-56, Aug. 28, 1991.

Financial Markets: Active Oversight of Market Automation by SEC and CFTC Needed, GAO/IMTEC-91-21, May 10, 1991.

Stock Market Automation: Exchanges Have Increased Systems' Capacities Since the 1987 Market Crash, GAO/IMTEC-91-37, May 10, 1991.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. VISA and MasterCard credit cards are also accepted.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:
U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

Orders by visiting:
Room 1100
700 4th St., NW (corner of 4th and G Sts. NW)
Washington, DC 20013

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
TDD (202) 512-2537

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

Orders by Internet
For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

- Web site: http://www.gao.gov/fraudnet/fraudnet.htm
- E-mail: fraudnet@gao.gov
- 1-800-424-5454 (automated answering system)

PRINTED ON RECYCLED PAPER